

# UNITED STATES DISTRICT COURT

for the  
District of Nebraska

In the Matter of the Search of

Apple iPhone (IMEI: 353891100367262) and Apple iPhone (IMEI: 356428101489261)  
(hereinafter "Subject Electronics") seized during a Search Warrant at 7602 Hinds Avenue,  
North Hollywood, California and currently in Lancaster County Sheriff's Office (LSO)  
custody and control at LSO in Lincoln, Nebraska.

Case No. 8:24MJ457

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment A (incorporated by reference).

located in the \_\_\_\_\_ District of \_\_\_\_\_ Nebraska \_\_\_\_\_, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B (incorporated by reference).

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 USC 841	Possession of Controlled Substances
21 USC 846	Conspiracy to Distribute Controlled Substances
18 USC 1956	Money Laundering

The application is based on these facts:

See Attached Affidavit in Support of an Application for a Search Warrant.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



*Applicant's signature*

Tyler Loos, Task Force Officer with HSI

*Printed name and title*

Sworn to before me by telephone or other  
reliable electronic means

Date: 11/19/2024

City and state: Omaha, Nebraska



*Judge's signature*

MICHAEL D. NELSON, U.S. Magistrate Judge

*Printed name and title*

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Tyler Loos, a Task Force Officer with Homeland Security Investigations, being duly sworn, depose and state as follows:

**INTRODUCTION**

I am a Task Force Officer with Homeland Security Investigations (HSI). I have been a Task Force Officer with HSI, formerly U.S. Immigration and Customs Enforcement, since March 2022. I have been employed with the Lancaster County Sheriff's Office in Lincoln, Nebraska since April 2014. During this time, I have served in the capacity of a patrol deputy from 2014 to 2017, General Investigator from 2017 to 2019, Special Victims Investigator from 2019 to 2022, and currently serve as a Technical Investigator. I have extensive experience in relation to the investigation of various crimes, including but not limited to; homicides, sexual assaults, child abuse, white collar offenses, identity fraud, organized criminal enterprises involving illegal narcotics, and other organized criminal enterprises. I am currently assigned to the HSI Office in Omaha, Nebraska. In connection with my duties and responsibilities as a Task Force Officer, I have been involved in investigations of individuals who derive substantial income from the importation, manufacture, distribution and sale of illegal controlled substances. I have experience in the execution of search and arrest warrants, debriefing of defendants, informants, witnesses and other persons who have personal knowledge of the amassing, spending, converting, transporting, distribution, laundering, and concealing of proceeds of controlled substances trafficking. These investigations have resulted in the arrest and conviction of individuals who have used communications facilities to facilitate drug trafficking activity, and of individuals who laundered proceeds derived from drug trafficking activity. These

investigations have resulted in seizures of illegal drugs and proceeds derived from drug trafficking activity. These investigations have also required the examination of telephone records, forensic extraction of numerous electronic devices, financial records, drug ledgers and other documents.

Based on my training and experience and based upon interviews with defendants, informants, and other witnesses and participants in drug trafficking activity, I am familiar with the ways drug traffickers conduct their business. My familiarity includes: the means and methods drug traffickers use to import and distribute drugs; their use of cellular telephones and calling cards to facilitate drug activity; and their use of numerical codes and code words to conduct drug transactions. I also am familiar with how drug traffickers conceal, convert, transmit, and transport their drug proceeds, including but not limited to, using carriers to transport currency and proceeds, and using third parties to purchase or hold title to assets.

The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

I make this affidavit in support of an application for a search warrant to authorize the examination of property seized during a Search Warrant at 7602 Hinds Avenue, North Hollywood, California, to include: Apple iPhone (IMEI: 353891100367262) and Apple iPhone (IMEI: 356428101489261) (hereinafter “**Subject Electronics**”). The **Subject Electronics** are currently in Lancaster County Sheriff’s Office (LSO) custody and control at LSO in Lincoln, Nebraska. Based on the facts set forth in this affidavit, I believe probable cause exists for the issuance of a warrant to search the **Subject Electronics**, identified in **Attachment A** of this

affidavit, for contraband, the fruits of a crime, or things otherwise criminally possessed; or intended for use or which is or has been used as the means for committing a criminal offense, namely, of 21 USC 841, possession and 21 USC 846 conspiracy to distribute narcotics and 18 USC 1956 Money Laundering, as described in **Attachment B**.

The statements contained in this affidavit are based upon my investigation, information provided by other law enforcement officers, other personnel specially trained in the seizure and analysis of computers and electronic media, and on my experience and training as a Technical Investigator and Task Force Officer with HSI. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of the violations of 21 USC 841, possession and 21 USC 846 conspiracy to distribute narcotics and 18 USC 1956 Money Laundering, will be located in the **Subject Electronics**.

### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

As described above and in **Attachment B**, this application seeks permission to search for records that might be found in the **Subject Electronics**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B). Searches and seizures of evidence from computers commonly require investigators to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, computer related documentation, and

peripherals) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto optical, and others) can store the equivalent of thousands of pages of information.

Especially when the user wants to conceal criminal evidence, he or she often stores it in random order and with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

### **SEARCH METHODOLOGY TO BE EMPLOYED**

The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is

a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment B**; and/or
- g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment B**.

## **PROBABLE CAUSE**

On September 12, 2019, the Lancaster County Sheriff's Office (LSO) Interdiction Unit arrested Tyler Gooch (W/M 5-20-1980) at NW 84 & HWY 34, Lincoln, Lancaster County, Nebraska, after the vehicle he was driving was found containing 90 pounds of marijuana, 3,001 THC vape cartridges, and 30 pounds of marijuana shatter.

The investigation was continued by the Homeland Security Investigations Major Crimes Financial Task Force (MCFTF) made up of Lancaster County Sheriff's Office Investigators, Nebraska State Patrol Investigators, and Agents from the Department of Homeland Security Investigations, Omaha Field Office.

Through the investigation, it was later determined that the controlled substances Gooch was in possession of were going to be delivered to a cooperating defendant (CD-1) of known reliability in eastern Nebraska.

On January 19, 2020, law enforcement surveillance observed CD-1 meet with two males in a gold Ford Sport Trac outside of a Papillion NE residence, where the Ford Sport Trac was observed parking inside the garage of the residence. Shortly thereafter, surveillance officers followed the Ford Sport Trac after it departed the Papillion residence.

After leaving the Papillion residence, MCFTF Investigators observed the gold Ford Sport Trac traveling eastbound on Interstate 80 near mile marker 448 in Omaha, Douglas County, Nebraska. Investigators observed the Ford Sport Trac fail to signal a lane change and following another vehicle too closely.

A traffic stop was initiated on the gold Ford Sport Trac and contact was made with the two male occupants. The driver was identified as Frederick ROBEY (W/M 4-28-1976) and the passenger was identified as Eric Osborne THIBODO (W/M 5-31- 1968). Consent to search the vehicle was denied so a State of Nebraska certified K9 was deployed and alerted and indicated to the odor of narcotics emitting from within the vehicle. A probable cause search of the Ford Sport Trac was conducted and \$200,403.00 in US Currency was found in a black plastic trash bag. The

US Currency was rubber banded together in bundles and had a strong odor of marijuana emitting from them and from the bag. The US Currency pretested positive for THC. Officers also seized multiple phones from ROBEY and THIBODO.

Pursuant to a signed Lancaster County Court search warrant, investigators analyzed THIBODO's iPhone X using telephone number 213-808-4416 and his eTalk phone using telephone number 786-526-4267 that were seized during the January 19, 2020, traffic stop. During the phone analysis, investigators observed THIBODO's phone to have a messaging application named 'Wickr.' The Wickr application is known to investigators to be encrypted and is commonly used by persons to communicate covertly. Through previous training and experience, your Affiant knows persons involved in conspiracies often utilize encrypted cell phone applications to anonymize their identity when communicating with co-conspirators.

An analysis of the cellular telephone devices seized from THIBODO revealed that CD-1, Evan BOWEN and THIBODO communicated via cellular telephone and Wickr App. During these conversations, BOWEN used a name "EVANDER707". During the analysis of THIBODO'S personal cellular telephone 213-808-4416 and CD-1 cellular telephone, it was revealed that, THIBODO, BOWEN, and CD-1 were discussing the delivery of narcotics from Chicago, Illinois to Omaha, Nebraska.

Concurrent to the stop of the Ford Sport Trac, a search warrant was executed at the Papillion, NE residence the Ford Sport Trac was seen leaving. Pursuant to the search warrant, Investigators seized approximately 111 pounds of marijuana, 32 pounds of THC shatter, and 5 pounds of THC oil from within the Papillion residence. CD-1 was arrested at the Papillion residence and his phone was seized.

A search of his phone revealed that between January 16, 2020, through January 19, 2020, CD-1 and BOWEN discussed, on SMS messages, the purchase and delivery of narcotics from BOWEN to CD-1 in Omaha, Nebraska. BOWEN messaged CD-1 that a "Really good friend of mine will be supervising this trip to make sure it goes well. Please take good care of him. Need him to be safe. Big part of my operation."



HSI interviewed CD-1 after his arrest who stated that THIBODO was the subject who delivered the approximately 111 pounds of marijuana, 32 pounds of THC shatter, and 5 pounds of THC oil on January 19, 2020. CD-1 stated that he had ordered the marijuana products from BOWEN. CD-1 identified pictures of THIBODO. CD-1 also admitted that the narcotics found in Tyler Gooch's possession on September 12, 2019, was being delivered to him.

Through the examination of THIBODO's seized phone, HSI was able to identify several drug messages to different phone numbers of other co-conspirators. On January 6, 2020, "Katie" with phone number 323-723-3287 sent a group of messages to THIBODO asking if he was turning anything in this week and making the comment that they keep missing each other. Katie went on to send the text, "Lincoln, Nebraska correct". THIBODO responded, "Yes dear." THIBODO continued to discuss "paper" pickup with Katie through several text messages. Based on your affiant's training and experience, these discussions are code for the delivery of narcotics and pick up of currency.

In February 2020, LSO subpoenaed phone records for THIBODO's telephone number 213-808-4416. An analysis of the records determined that after the MCFTF seized THIBODO's Apple iPhone X using 213-808-4416, THIBODO purchased an iPhone 11 Pro with IMEI number 353234103868939, and continued using number 213-808-4416.

On March 24, 2020, pursuant to a Lancaster County, Nebraska warrant, electronic surveillance was established on THIBODO's Apple iPhone 11 Pro using phone number 213-808-4416, and revealed that THIBODO traveled to the New York City metro area. Electronic surveillance placed THIBODO's phone near a warehouse located at 5819 58th Road, Maspeth, New York that was being leased by the company FastBox, LLC.

Research on the company FastBox LLC revealed it to have office warehouses in New York, New York, Nashville, Tennessee, Laurel, Maryland, Cincinnati, Ohio, North Hollywood, California, Chicago, Illinois, and Miramar, Florida. Additional research has revealed limited information about the business FastBox LLC. FastBox LLC advertises on their website, (<https://www.goFastBox.com/>) that FastBox LLC was born to provide an alternative to

traditional portable storage moving solutions. In late March 2020, 24 hours electronic surveillance was established on multiple FastBox warehouses, to include Maspeth, New York and North Hollywood, California. Analysis of historic phone records including both of the **Subject Electronics** was completed by members of the law enforcement task force, which shows co-conspirators, to include “Junior” AKA Gabriel COLINDRES have all been in the area of the Fast Box LLC warehouse locations in different parts of the United States. The investigation has revealed no evidence that FastBox did any legitimate business. This has been confirmed by several cooperating defendants.

On April 11, 2020, a worker at the FastBox New York City location was observed through electronic surveillance moving wooden FastBox crates from the FastBox NY warehouse into a third-party semi-tractor bearing New York plate 712157PC towing trailer bearing Maine licenses plate 2280450.

On April 13, 2020, the HSI Oklahoma City Task Force officer stopped the semi tractor bearing New York plate 712157PC towing trailer bearing Maine licenses plate 2280450 after the semi was observed failing to maintain its lane of travel. After a canine alerted and indicated to the odor of narcotics coming from within the trailer, a probable cause search of the trailer, HSI discovered approximately \$3.9 million of suspected narcotics proceeds secreted in one of the FastBox crates. The suspected narcotics proceeds were packaged and marked with different symbols and/or acronyms, which made your affiant believe the bulk currency belonged to different individuals.

On or about May 7, 2020, HSI executed multiple search warrants on FastBox locations, FastBox containers, FastBox employee’s residence and FastBox storage units in California, Chicago, Cincinnati, Kansas City and New York. Pursuant to the warrants, HSI New York, HSI Cincinnati, HSI Chicago, HSI Kansas City and HSI California seized over 55,000 vials of Marijuana biproduct tetrahydrocannabinol (THC) vape pens, which is equivalent to approximately 3500 kilograms of dried leave marijuana and over \$1.6 million of suspected narcotics proceeds. HSI also seized cell phones used by employees of the FastBox warehouses.

Of the locations searched on or about May 7, 2020, 7602 Hinds Ave in North Hollywood, California was included. Through physical and electronic surveillance, HSI Los Angeles previously identified this location as a residence frequented by Gabriel COLINDRES. During the search of COLINDRES' bedroom at 7602 Hinds Ave, several shoe boxes and two safes were located. A large amount of US currency was located within two separate boxes. There were four pieces of paper in one of the boxes. Three of the four pieces of paper had "Wally" written on them, along with numeric amounts. US currency was also located in one of the safes. Additional US currency was located within two boxes under a chair in COLINDRES' bedroom.

During the search warrant at 7602 Hinds Ave, COLINDRES stated the master bedroom was his bedroom, which is where a large amount of US currency was located. COLINDRES engaged in conversation with agents, and stated he has worked construction since the age of 18, further adding the currency does not belong to anyone else. COLINDRES did sign a Notice of Abandonment form for the US currency. The amount of US currency seized from 7602 Hinds Ave totaled \$620,499.

Currency seized by HSI in Oklahoma City on April 13, 2020 also had the name "Wally." Your Affiant knows "Wally" is Richard Wesley MARSHALL. On May 7, 2020, while executing California state search warrant at 7602 Hinds Ave, COLINDRES was detained for questioning. In COLINDRES' possession were the Two Apple iPhones (**Subject Electronics**).

In June 2020, a Lancaster County subpoena Duces Tecum was served on Verizon wireless for Two Apple iPhones (**Subject Electronics**). Subscriber recorders for Apple iPhone (IMEI: 353891100367262) listed COLINDRES as the subscriber to this phone; whereas Apple iPhone (IMEI: 356428101489261) was listed as a prepaid phone with the number 323-240-4248 assigned.

In May 2020, a Nebraska State Search warrant authorizing the search of an Apple iPhone 6S seized from Michael GARRINGER, a co-conspirator who worked for the LEIDERMAN/REJA DTO. Signal messages located in the GARRINGER iPhone 6S has "JR"

listed as the owner of 323-240-4248. Your affiant through my training and experience in digital phone forensic believes the Two Apple iPhones (**Subject Electronics**) belong to COLINDRES.

HSI Omaha confirmed with West Covina detectives who were present at the search warrant 7602 Hinds Ave, that everyone in the home denied ownership of the Two Apple iPhones (**Subject Electronics**). Through my training and experience, your affiant knows suspects and non-suspects routinely distance themselves from ownership of items if they aren't the owners or if they know the item may contain illegal activity.

In May 2020, LSO conducted forensic analysis of the phones seized from members/employees of FastBox. Text messages and audio messages discovered during the analysis indicate FastBox members/employees were under the direction of David Max LEIDERMAN (W/M 3-12-75). Text conversations and audio clips were identified as belonging to LEIDERMAN based on voice comparisons and a third cooperating defendant (CD-3) who identified messages coming from LEIDERMAN. The messages gave instructions to FastBox members/employees on how shipments should be made and persons that could be trusted. Based on your affiant's training and experience and the stern tone of the messages, your affiant believes LEIDERMAN was in charge of the organization.

The analyzed text messages from the seized phones of FastBox members/employees along with subpoenaed bank records for FastBox bank accounts, indicated bulk cash of approximately \$1.4 million were deposited by members/employees between 2017 and 2020. Members/ employees of the organization would deposit small, predetermined amounts into FastBox accounts via ATM at multiple banks in the Los Angeles California area.

Subpoenaed records for the third-party transportation companies used by FastBox LLC to ship FastBox crates indicated FastBox shipped approximately 247 loads from California between 2014 and 2020. The records also indicated FastBox LLC shipped 368 loads to California between 2014 and 2020. To date the investigation has revealed no evidence that FastBox did any legitimate business. This has been confirmed by several cooperating defendants.

In May 2020, a second cooperating defendant (CD-2) who HSI has deemed credible and reliable confirmed that FastBox LLC began operations in 2014. CD 2 stated he was approached by LEIDERMAN and agreed to start FastBox in CD-2's name. CD-2 stated his job was to facilitate financial payments for all logistics for FastBox to maintain the appearance that FastBox was a legitimate moving company, but he soon realized the company conducted no legitimate business and was used to transport narcotics and narcotic proceeds. CD-2 has met with LEIDERMAN on several occasions over a six-year period. CD-2 identified a picture of LEIDERMAN as the person who asked CD-2 to start FastBox.

In May and June 2020, a third cooperating defendant (CD-3) who HSI has deemed credible and reliable, confirmed that FastBox LLC began operations in 2014 as a marijuana and marijuana byproduct delivery company. CD-3 also confirmed that LEIDERMAN and James Vincent REJA (W/M 06-25-1974) were partners in charge of the operation. CD-3 indicated THIBODO was a client of LEIDERMAN and REJA, who used the FastBox service to move marijuana and marijuana proceeds between California and the other FastBox locations. CD-3 identified pictures of LEIDERMAN, REJA, and THIBODO. CD-3 informed investigators COLINDRES would work with clients regarding the pick up of marijuana and distribute the narcotics proceeds. CD-3 stated COLINDRES managed the Los Angeles Fast Box location which included picking up marijuana product from clients of the LEIDERMAN/REJA DTO and loading them onto the Fastbox containers to be shipped around the country. CD-3 stated COLINDRES was also responsible for distributing the marijuana proceeds to the clients once the proceeds arrived in Los Angeles.

CD-3 stated that since 1998, he had been working with LEIDERMAN and REJA in various roles in the DTO. Originally CD-3 started working in marijuana grow locations in California tending to the growth of marijuana plants. Later, CD-3 moved to New York and started receiving large shipments of marijuana and marijuana products for delivery. CD-3 would then ship the money back to LA for LEIDERMAN and REJA. During this time CD-3 would contact LEIDERMAN and REJA for instructions concerning the business. CD-3 stated that

LEIDERMAN and REJA were equal partners but had different roles within the DTO. HSI Omaha recorded conversations between CD-3 and LEIDERMANN, and CD-3 and REJA, discussing the FastBox transportation business. CD-3 estimated LEIDERMANN and REJA produced over 1,000,000 pounds of marijuana between 1998 and 2014, the majority shipped to New York City. CD-3 estimated each bulk currency shipment from New York to California in the FastBox containers was at least \$1,000,000. CD-3 indicated the container that was seized on April 13, 2020, was a larger shipment.

CD-3 indicated “A”/“A-Real” a/k/a Adam BREGMAN, THIBODO aka “NYO”, and “Wally” a/k/a Richard Wesley MARSHALL were clients of LEIDERMAN and REJA who used the FastBox service to move marijuana and marijuana proceeds between California and the other FastBox locations.

Through the investigation your affiant has learned that LEIDERMANN, BOWEN, THIBODO, BREGMAN, MARSHALL, COLINDRES and REJA used their electronic devices to communicate with other members of the organization to further their narcotics trafficking and money laundering activities. It is believed that evidence of narcotics trafficking, and money laundering will be stored within the **Subject Electronics**. **The Subject Electronics** seized are “smart” devices capable of storing large amounts of date, time, and location specific information and data, including call details, text messaging, contact information, audio and video files, pictures, global position information, chat messaging, email, voice mail messaging, web browsing history, wireless network access history, document files, application databases, etc.

### CONCLUSION

Based upon the facts set forth in this affidavit, I believe that there is probable cause to believe that violations of Title 21, United States Code, Sections 841 and 846; and violations of Title 18, United States Code 1956; and that evidence of those violations, which is more fully

described in **Attachment B** to this affidavit, exist in the **Subject Electronics**, which is more fully described in **Attachment A** to this affidavit.

This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. § 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated.

Respectfully submitted,



Tyler Loos, Task Force Officer  
U.S. Department of Homeland Security

Sworn to before me by reliable electronic means:

Date: 11/19/2024

City and State: Omaha, Nebraska



Michael D. Nelson, U.S. Magistrate Judge



**ATTACHMENT A**

**DESCRIPTION OF PROPERTY TO BE SEARCHED “Subject Electronics”**

Apple iPhone (IMEI: 353891100367262) seized from 7602 Hinds Avenue, North Hollywood, California which is currently stored at the Lancaster County Sheriff's Office in Lincoln, Nebraska. The search of these devices will take place in the District of Nebraska.





Apple iPhone (IMEI: 356428101489261) seized from 7602 Hinds Avenue, North Hollywood, California, which is currently stored at the Lancaster County Sheriff's Office in Lincoln, Nebraska. The search of these devices will take place in the District of Nebraska.



**ATTACHMENT B**  
**ITEMS TO BE SEIZED**

1. All records on the **Subject Electronics**, described in Attachment A that relate to violations of Title 21 U.S.C. Section 841(b)(1)(C) and Title 21 U.S.C. Section 841(b)(1), that involve DEFENDANT(s) NAME, and/or their co-conspirators:

- a. lists of customers and related identifying information;
- b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
- d. any information recording schedule or travel.
- e. all bank records, checks, credit card bills, account information, and other financial records;
- f. any information relating to wire transfers of funds.

2. Evidence of user attribution showing who used or owned the **Subject Electronics** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and Internet browsing history;

3. Records of Internet activity from any Internet browser used on the **Subject Electronics** relating to Items 1 and 2 above, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

5. Evidence of other accounts associated with this device including email addresses, social media accounts, messaging “app” accounts, and other accounts that may be accessed through the digital device that will aid in determining the possessor/user of the **Subject Electronics**;

6. Evidence of use of the **Subject Electronics** to communicate with others about the above-listed crime(s), via email, chat sessions, instant messages, text messages, app communications, social media, internet usage, and other similar digital communications;

7. Photographs, images, videos, documents, and related data created, accessed, read, modified, received, stored, sent, moved, deleted or otherwise manipulated;
8. Evidence of use of the **Subject Electronics** to conduct internet searches relating to above listed crime(s);
9. Information that can be used to calculate the position of the **Subject Electronics** between the above dates, including location data; GPS satellite data; GPS coordinates for routes and destination queries between the above-listed dates; “app” data or usage information and related location information; IP logs or similar internet connection information, and images created, accessed or modified between the above-listed dates, together with their metadata and EXIF tags;
10. Evidence of the identity of the person in possession of the **Subject Electronics** and the associated times and dates. Such evidence may be found in digital communications, photos and video and associated metadata, IP logs, documents, social media activity, and similar data;
11. Records linking the suspect(s), co-conspirators, victim(s), witness(es) to a certain screen name, handle, email address, Social media identity, etc.;
12. Records showing a relationship with victim(s), location(s), other suspects, etc.;
13. Names, nicknames, account ID’s, phone numbers, or addresses of specific persons;
14. Records showing a relationships to particular areas or locations.;
15. Photographs, images, videos, documents that contain or are evidence of above listed crime(s);
16. Evidence of purchases, such as items used in planning or carrying out above listed crimes(s);
17. Internet research history conducted while planning, executing, or covering up to commit above listed crimes(s);
18. Any live and deleted user attribution data including user accounts, e-mail accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data storage accounts, documents, files, calendars, metadata, recycle bin files, and any other information and evidence that may demonstrate attribution to a particular user or users of **Subject Electronics**;
19. Any live and deleted applications, programs, or software, used to facilitate the creation, storage, display, or transmission of digital visual recordings and the logs and data associated with the applications, programs or software, and any **Subject Electronics** backup files;
20. Any live and deleted audio or visual recording files including files bearing file extensions jpg, jpeg, png, gif, tif, wav, aiff, mp3, mp4, avi, mpg, mpeg, flv, mp4, mov, and wmv along with any descriptive metadata within or associated with the visual recording files, which may include

date and time the recording was created, the **Subject Electronics** used to create the recording and location the recording was made

## UNITED STATES DISTRICT COURT

for the  
District of Nebraska

In the Matter of the Search of

)  
)  
) Apple iPhone (IMEI: 353891100367262) and Apple iPhone (IMEI: 356428101489261)  
) (hereinafter "Subject Electronics") seized during a Search Warrant at 7602 Hinds Avenue,  
) North Hollywood, California and currently in Lancaster County Sheriff's Office (LSO)  
) custody and control at LSO in Lincoln, Nebraska.  
)

Case No. 8:24MJ457

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_ Nebraska

(identify the person or describe the property to be searched and give its location):

See Attachment A (incorporated by reference).

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B (incorporated by reference).

**YOU ARE COMMANDED** to execute this warrant on or before December 3, 2024 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Michael D. Nelson.

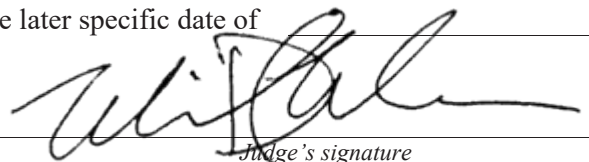
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

11/19/2024 4:23 pm

Date and time issued:



Judge's signature

City and state:

Omaha, Nebraska

MICHAEL D. NELSON, U.S. Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**Case No.:  
8:24MJ457

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*



**ATTACHMENT A**

**DESCRIPTION OF PROPERTY TO BE SEARCHED “Subject Electronics”**

Apple iPhone (IMEI: 353891100367262) seized from 7602 Hinds Avenue, North Hollywood, California which is currently stored at the Lancaster County Sheriff's Office in Lincoln, Nebraska. The search of these devices will take place in the District of Nebraska.



Apple iPhone (IMEI: 356428101489261) seized from 7602 Hinds Avenue, North Hollywood, California, which is currently stored at the Lancaster County Sheriff's Office in Lincoln, Nebraska. The search of these devices will take place in the District of Nebraska.





**ATTACHMENT B**  
**ITEMS TO BE SEIZED**

1. All records on the **Subject Electronics**, described in Attachment A that relate to violations of Title 21 U.S.C. Section 841(b)(1)(C) and Title 21 U.S.C. Section 841(b)(1), that involve DEFENDANT(s) NAME, and/or their co-conspirators:
  - a. lists of customers and related identifying information;
  - b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
  - c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
  - d. any information recording schedule or travel.
  - e. all bank records, checks, credit card bills, account information, and other financial records;
  - f. any information relating to wire transfers of funds.
2. Evidence of user attribution showing who used or owned the **Subject Electronics** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and Internet browsing history;
3. Records of Internet activity from any Internet browser used on the **Subject Electronics** relating to Items 1 and 2 above, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
4. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.
5. Evidence of other accounts associated with this device including email addresses, social media accounts, messaging “app” accounts, and other accounts that may be accessed through the digital device that will aid in determining the possessor/user of the **Subject Electronics**;
6. Evidence of use of the **Subject Electronics** to communicate with others about the above-listed crime(s), via email, chat sessions, instant messages, text messages, app communications, social media, internet usage, and other similar digital communications;

7. Photographs, images, videos, documents, and related data created, accessed, read, modified, received, stored, sent, moved, deleted or otherwise manipulated;
8. Evidence of use of the **Subject Electronics** to conduct internet searches relating to above listed crime(s);
9. Information that can be used to calculate the position of the **Subject Electronics** between the above dates, including location data; GPS satellite data; GPS coordinates for routes and destination queries between the above-listed dates; “app” data or usage information and related location information; IP logs or similar internet connection information, and images created, accessed or modified between the above-listed dates, together with their metadata and EXIF tags;
10. Evidence of the identity of the person in possession of the **Subject Electronics** and the associated times and dates. Such evidence may be found in digital communications, photos and video and associated metadata, IP logs, documents, social media activity, and similar data;
11. Records linking the suspect(s), co-conspirators, victim(s), witness(es) to a certain screen name, handle, email address, Social media identity, etc.;
12. Records showing a relationship with victim(s), location(s), other suspects, etc.;
13. Names, nicknames, account ID’s, phone numbers, or addresses of specific persons;
14. Records showing a relationships to particular areas or locations.;
15. Photographs, images, videos, documents that contain or are evidence of above listed crime(s);
16. Evidence of purchases, such as items used in planning or carrying out above listed crimes(s);
17. Internet research history conducted while planning, executing, or covering up to commit above listed crimes(s);
18. Any live and deleted user attribution data including user accounts, e-mail accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data storage accounts, documents, files, calendars, metadata, recycle bin files, and any other information and evidence that may demonstrate attribution to a particular user or users of **Subject Electronics**;
19. Any live and deleted applications, programs, or software, used to facilitate the creation, storage, display, or transmission of digital visual recordings and the logs and data associated with the applications, programs or software, and any **Subject Electronics** backup files;
20. Any live and deleted audio or visual recording files including files bearing file extensions jpg, jpeg, png, gif, tif, wav, aiff, mp3, mp4, avi, mpg, mpeg, flv, mp4, mov, and wmv along with any descriptive metadata within or associated with the visual recording files, which may include

date and time the recording was created, the **Subject Electronics** used to create the recording and location the recording was made